保型形式の合同とその応用について (代数的整数論とその周辺)

千田, 雅隆

数理解析研究所講究録 1376 巻 2004 年 61-71

保型形式の合同とその応用について

東北大学大学院理学研究科 千田 雅隆 (Masataka Chida)
Institute of Mathematics, Tohoku University

1 Introduction

Kohnen-Ono [7] は半整数 weight の保型形式の理論及び保型形式の合同に関する性質をうまく使うことにより, 5 以上の素数 p に対して,

$$\#\{D \in S(X) \mid 0 < D,\ p \nmid h(\mathbb{Q}(\sqrt{-D}))\} \gg_p \frac{\sqrt{X}}{\log X}$$

が成り立つことを示した. ここで $h(K)$ は K の類数とし,

$$S(X) := \{D \in \mathbb{Z} \mid |D| < X,\ D \text{ は square-free}\}$$

とする.

さらに Byeon [1] は Kohnen-Ono が使った手法を精密化することにより,

$$\#\{D \in S(X) \mid 0 < D,\ \lambda_p(\mathbb{Q}(\sqrt{-D})) = 0\} \gg_p \frac{\sqrt{X}}{\log X}$$

を示した. ここで $\lambda_p(k)$ は k の円分 $\mathbb{Z}_p$-拡大に関する岩澤 λ-不変量とする.

本稿では Byeon の結果の楕円曲線版について紹介する. E を Weierstrass 方程式

$$E : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{Z})$$

によって定まる $\mathbb{Q}$ 上の楕円曲線とし, square-free な整数 $D \neq 0$ に対し E_D を

$$E_D : y^2 = x^3 + aD^2x + bD^3$$

により定まる楕円曲線とする. E_D は E の D による quadratic twist と呼ばれる. Kohnen-Ono [7] 及び James-Ono [5] の結果によって, 十分大きな素数 p に対して

$$\#\{D \in S(X) \mid \operatorname{rank} E_D(\mathbb{Q}) = 0,\ \#\text{Ш}(E_D/\mathbb{Q})_p = 1\} \gg_{E,p} \frac{\sqrt{X}}{\log X}$$

となることが知られている. ここで $\text{Ш}(E/\mathbb{Q})_p$ は $E/\mathbb{Q}$ の Tate-Shafarevich 群の p-part とする. この定理を示すのに使われた手法を応用することにより, 次の結果が得られた.

定理 1.1 Eを有理数体上の楕円曲線とする．このとき$1+p-\#\tilde{E}(\mathbb{F}_p) \notin \{-1,0,+1\}$を満たす十分大きな素数$p$に対して

$$\#\{D \in S(X) \mid \lambda^{\mathrm{anal}}_{E_D,p} = \mu^{\mathrm{anal}}_{E_D,p} = 0\} \gg_{E,p} \frac{\sqrt{X}}{\log X}$$

が成り立つ．ここで $\lambda^{\mathrm{anal}}_{E,p}$, $\mu^{\mathrm{anal}}_{E,p}$ はEのp進L関数に関する岩澤不変量を表す．

注 1.2 Kato や Kolyvagin の結果により，$\lambda^{\mathrm{anal}}_{E_D,p} = \mu^{\mathrm{anal}}_{E_D,p} = 0$ ならば $\lambda^{\mathrm{alg}}_{E_D,p} = \mu^{\mathrm{alg}}_{E_D,p} = 0$ となることが知られている．ただし $\lambda^{\mathrm{alg}}_{E,p}$, $\mu^{\mathrm{alg}}_{E,p}$ はEのSelmer 群に関する岩澤不変量を表すこととする．よって，このときはEの Selmer 群に関する岩澤多項式とEのp進L関数に関する岩澤多項式はそれぞれ自明になるため，この場合は岩澤主予想が成り立つことが分かる．

注 1.3 Eがpで supersingular reduction を持つ場合でも Kobayashi の$(\pm)$ Selmer 群と Pollack の$(\pm)$ p進L関数に対して同様のことが証明できる．(このことを指摘していただいた栗原将人先生に感謝いたします)

2 楕円曲線の岩澤不変量

ここで楕円曲線に関する岩澤不変量について簡単に述べておく．Kは有理数体の代数拡大体でEをK上の楕円曲線とする．さらに $\mathrm{Sel}(E/K)$をE/Kの Selmer 群とする．いまpを奇素数としEはpで good ordinary reduction を持つと仮定する．また，$\mathbb{Q}_\infty/\mathbb{Q}$を $\mathbb{Q}$の円分$\mathbb{Z}_p$-拡大とし，$\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$ 及び$\Lambda = \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$とおけば，$\mathrm{Sel}(E/\mathbb{Q}_\infty)$ はΓ-moduleであり，そのp-primary subgroup $\mathrm{Sel}(E/\mathbb{Q}_\infty)_p$ はΛ-moduleとなる．このとき

$$X_E(\mathbb{Q}_\infty) = \mathrm{Hom}(\mathrm{Sel}(E/\mathbb{Q}_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$$

とおくと$X_E(\mathbb{Q}_\infty)$は有限生成torsion Λ-moduleとなることが知られている．

このことよりΛ-moduleの構造定理によって

$$X_E(\mathbb{Q}_\infty) \sim (\bigoplus_{i=1}^{n} \Lambda/(f_i(T)^{a_i})) \oplus (\bigoplus_{j=1}^{m} \Lambda/(p^{\mu_j}))$$

と書くことができる．ただしf_iはdistinguishedな多項式でありa_i, μ_jは正の整数とする．このときEの Selmer 群に関する岩澤不変量を

$$\begin{aligned} \lambda^{\mathrm{alg}}_{E,p} &= \sum_{i=1}^{n} a_i \deg(f_i(T)), \\ \mu^{\mathrm{alg}}_{E,p} &= \sum_{j=1}^{m} \mu_j \end{aligned}$$

によって定義する．さらに E の Selmer 群に関する岩澤多項式を

$$f_{E,p}^{\mathrm{alg}}(T) = p^{\mu_{E,p}^{\mathrm{alg}}} \prod_{i=1}^{n} f_i(T)^{a_i}$$

によって定義する．次に E の p 進 L 関数に関する岩澤不変量を定義する．いま，埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ をひとつ fix する．

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

を E の Hasse-Weil L 関数とし α_p, β_p を $\alpha_p\beta_p = p$, $\alpha_p + \beta_p = a(p)$ の解とする．ただし α_p は p 進単数となるように選ぶとする．

定理 2.1 (Mazur, Swinnerton-Dyer [10]) 次を満たすような $F_{E,p}(T) \in \mathbb{Q}_p[[T]]$ が存在する．

(i) $F_{E,p}(0) = (1 - \alpha_p^{-1})^2 L(E/\mathbb{Q}, 1)/\Omega_E$.
(ii) conductor が p^n であるような非自明な指標 $\rho : \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \to \overline{\mathbb{Q}}_p$ に対し，

$$F_{E,p}(\zeta - 1) = \tau(\rho^{-1})\beta_p^m L(E/\mathbb{Q}, \rho, 1)/\Omega_E$$

となる．

ただし ζ は 1 の原始 p^{n-1} 乗根，τ は Gauss 和，Ω_E は E の実周期であり，$L(E/\mathbb{Q}, \rho, s)$ は $L(E/\mathbb{Q}, s)$ の指標 ρ による twist とする．

p 進 Weierstrass の準備定理によって，$F_{E,p}(T)$ は

$$F_{E,p}(T) = p^{\mu} u(T) f(T)$$

という形に一意的に表わすことができる．ここで μ は有理整数，$u(T)$ は Λ の可逆元であり $f(T)$ は distinguished な多項式とする．このとき E の p 進 L 関数に関する岩澤不変量を

$$\begin{aligned} \lambda_{E,p}^{\mathrm{anal}} &= \deg(f(T)), \\ \mu_{E,p}^{\mathrm{anal}} &= \mu \end{aligned}$$

によって定義する．さらに E の p 進 L 関数に関する岩澤多項式を

$$f_{E,p}^{\mathrm{anal}}(T) = p^{\mu_{E,p}^{\mathrm{anal}}} f(T)$$

によって定める．このとき岩澤主予想は次のように述べられる．

予想 2.2 (Mazur)

$$f_{E,p}^{\mathrm{alg}}(T) = f_{E,p}^{\mathrm{anal}}(T).$$

この予想に対して現在では Kato [6] によって

$$f_{E,p}^{\mathrm{alg}}(T) \mid f_{E,p}^{\mathrm{anal}}(T) \text{ in } \mathbb{Q}_p[T]$$

となることが知られており, さらに E が虚数乗法を持つ場合には Rubin [12] によって岩澤主予想が成り立つことが証明されている.

注 2.3 定義により

$$F_{E_D,p}(0) = (1 - \left(\frac{D}{p}\right) \alpha_p^{-1})^2 L(E_D/\mathbb{Q}, 1)/\Omega_{E_D}$$

が p 進単数ならば $\lambda_{E_D,p}^{\mathrm{anal}} = \mu_{E_D,p}^{\mathrm{anal}} = 0$ となるので, 主定理を示すためにはこのような D がたくさん存在することを示せばよい.

3 半整数 weight の保型形式の理論

ここでは証明に必要な半整数 weight の保型形式の理論について紹介する. まず E_D の L 関数の値を調べるために次の定理を使う.

定理 3.1 (Ono-Skinner [11]) $E/\mathbb{Q}$ を conductor が M の楕円曲線とし, $\delta \in \{\pm 1\}$ を $L(E,s) = \sum_{n=1}^{\infty} a(n) n^{-s}$ の関数等式の符号とする. このとき次の (i),(ii),(iii) を満たす正の整数 N, mod N の Dirichlet 指標 χ, 複素数 $\Omega (\neq 0)$ 及び 0 でない eigenform

$$g(z) = \sum_{n=1}^{\infty} b(n) q^n \in S_{3/2}(N, \chi)$$

が存在する.

(i) $4M \mid N$.
(ii) $g(z)$ の志村対応での像が

$$F_E(z) = \sum_{n=1}^{\infty} a(n) q^n$$

のある指標による twist となる.
(iii) $\delta D > 0$ に対し

$$b(|D|)^2 = \begin{cases} \epsilon_D \frac{L(E_D,1)\sqrt{|D|}}{\Omega} & \text{if } (D,N) = 1, \\ 0 & \text{otherwise} \end{cases}$$

を満たす (ただし ϵ_D 及び $b(n)$ はある $\mathbb{Q}$ の有限次拡大体の代数的整数).

さらに D を $\delta D > 0$ 及び $(D, N) = 1$ を満たす整数とすれば，十分大きな素数 p に対し $|L(E_D, 1)/\Omega_{E_D}|_p = |b(|D|)^2|_p$ が成り立つ (ここで $|\cdot|_p$ は p 進付値とする).

この定理によって，主定理を証明するには $|b(D)|_p = 0$ となる D の個数を評価すればよいことがわかる．そのためには次の事実を用いる.

定理 3.2 (Sturm [15], Theorem 1)

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in M_k(N, \chi)$$

を重さが半整数 (または整数) weight の保型形式とし，その Fourier 係数 $a(m)$ はある代数体 K の整数であるとする．また，K の有限素点 v に対して

$$\mathrm{ord}_v(f) = \begin{cases} +\infty & \text{if } a(n) \equiv 0 \mod v \quad \text{for all } n, \\ \min\{\, n \mid a(n) \not\equiv 0 \mod v\} & \text{otherwise} \end{cases}$$

とおき，さらに

$$\lambda = \frac{k}{12}[\Gamma_0(1) : \Gamma_0(N)] = \frac{kN}{12}\prod_{p|N}\frac{p+1}{p}$$

とする．このとき $\mathrm{ord}_v(f) > \lambda$ ならば $\mathrm{ord}_v(f) = +\infty$ が成り立つ.

次の補題も非常に重要なものである.

補題 3.3 (Shimura [14])

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{k+1/2}(N, \chi)$$

を半整数 weight の cusp form とし l を素数とする．いま $(U_l f)(z)$ 及び $(V_l f)(z)$ を

$$\begin{aligned} (U_l f)(z) &= \sum_{n=1}^{\infty} u_l(n)q^n = \sum_{n=1}^{\infty} a(ln)q^n, \\ (V_l f)(z) &= \sum_{n=1}^{\infty} v_l(n)q^n = \sum_{n=1}^{\infty} a(n)q^{ln} \end{aligned}$$

と定義すれば，

$$\begin{aligned} (U_l f)(z) &\in S_{k+1/2}\left(Nl, \chi\left(\frac{4l}{\cdot}\right)\right), \\ (V_l f)(z) &\in S_{k+1/2}\left(Nl, \chi\left(\frac{4l}{\cdot}\right)\right) \end{aligned}$$

が成り立つ.

4 主定理の証明

ここでは定理 1.1 の証明を紹介する．講演では虚数乗法を持たない場合について紹介したが，ここでは虚数乗法を持つ場合について詳しく述べることにする．

補題 4.1 $E/\mathbb{Q}$ を楕円曲線, $L(E,s)=\sum_{n=1}^{\infty}a(n)n^{-s}$ をその L 関数とし，

$$f(z)=\sum_{n=1}^{\infty}a(n)q^n$$

を対応する保型形式とする．また，

$$g(z)=\sum_{n=1}^{\infty}b(n)q^n\in S_{3/2}(N,\chi)$$

を定理 3.1 により与えられる eigenform とする．さらに E は虚 2 次体 K による虚数乗法を持つとし，p は 3 より大きな素数とする．このとき負の整数 D_0 で $(D_0,N)=1$, $\epsilon=\left(\frac{D_0}{p}\right)\neq 0$ 及び $|b(|D_0|)|_p=1$ を満たすものが存在すれば

$$\#\left\{0<D\in S(X)\;\middle|\;\left(\frac{D}{p}\right)=\epsilon,\ |b(D)|_p=1\right\}\gg_{E,p}\frac{\sqrt{X}}{\log X}$$

が成り立つ．

証明

$$b_0(n)=\begin{cases}b(n) & \text{if } (n,Np)=1 \text{ and } \left(\frac{n}{p}\right)=\epsilon,\\ 0 & \text{otherwise}\end{cases}$$

とおけば

$$g_0(z)=\sum_{n=1}^{\infty}b_0(n)q^n\in S_{3/2}(Np^2,\chi')$$

であり，いま E は K により虚数乗法を持つので，$l\equiv 3 \mod 4$, $(l,N)=1$ 及び $\left(\frac{\Delta_K}{l}\right)=-1$ を満たす素数 l に対して $a(l)=0$ が成り立つ (ここで Δ_K は K の判別式)．このような l に対し，Hecke 作用素 $T(l^2)$ の作用を考えると

$$b(l^2n)+\chi'(l)\left(\frac{-n}{l}\right)b(n)+\chi'^2(l)lb(n/l^2)=0$$

となることがわかる．よって $(r,t)=1$, $4\,|\,t$, $r\equiv 3 \mod 4$ となる r, t に対し

$$\#T(r,t,X):=\#\{\,l:\text{素数}\,|\,l\le X,\ a(l)=0,\ l\equiv r \bmod t\}\gg_E\frac{X}{\log X}$$

であり， $l \in T(r,t) := \{\, l : 素数 \mid a(l) = 0,\, l \equiv r \bmod t\}$ とすれば

$$b(l^2 n) = \chi'(l)\left(\frac{n}{l}\right) b(n) - \chi'^2(l) l b(n/l^2) \tag{4.1}$$

となることがわかる.

ここで $\kappa = [\Gamma_0(1) : \Gamma_0(Np^2)]/8 + 1$ と置き，(r_0, t_0) を次を満たすように選ぶ.

(1) $Np^2 | t_0$, $(r_0, t_0) = 1$, $\chi'(r_0) = 1$ かつ $r_0 \equiv 3 \mod 4$ を満たす.
(2) $l \equiv r_0 \mod t_0$となる素数lに対し，$\left(\frac{n}{l}\right) = 1$ が任意の $1 \le n \le \kappa$, $(n, Np^2) = 1$ に対して成り立つ.
(3) $l \equiv r_0 \mod t_0$となる素数lに対し，$\left(\frac{\Delta_K}{l}\right) = -1$.
(4) $l \equiv r_0 \mod t_0$となる素数lに対し，$\left|\chi'(l^2) l - \chi'(l)\left(\frac{D_0}{l}\right)\right|_p = 1$.

いま $l \in T(r_0, t_0)$ を十分大きな素数とすると, 全ての $1 \le n \le \kappa$ に対して

$$u_l(ln) = b_0(l^2 n) = \chi'(l)\left(\frac{n}{l}\right) b_0(n) - l\chi'^2(l) b_0(n/l^2) = \chi'(l) b_0(n) = v_l(ln)$$

となることが分かり, さらに (4.1) より,

$$v_l(l^3|D_0|) = b_0(l^2|D_0|) = \chi'(l)\left(\frac{D_0}{l}\right) b_0(|D_0|),$$

$$u_l(l^3|D_0|) = b_0(l^4|D_0|) = -l\chi'(l^2) b_0(|D_0|)$$

となる. ここで (r_0, t_0) の選び方より,

$$u_l(l^3|D_0|) - \chi'(l) v_l(l^3|D_0|) = (\chi'(l^2) l - \chi'(l)\left(\frac{D_0}{l}\right)) b_0(|D_0|) \not\equiv 0 \mod p$$

なので

$$\mathrm{ord}_p(U_l g_0 - \chi'(l) V_l g_0) < +\infty$$

がわかる. 定理 3.2 と補題 3.3 より, ある正の整数 n_l が存在して

$$1 \le n_l \le [\Gamma_0(1) : \Gamma_0(Np^2 l)]/8 = \kappa(l+1),\ (n_l, l) = 1$$

かつ

$$b_0(n_l l) = u_l(n_l) \not\equiv \chi'(l) v_l(n_l) = 0 \mod p$$

となる. 以上から, D' を $D = n_l l$ の square-free part とするとき,

$$|b_0(D')|_p = 1$$

が成り立つ. さらに Chebotarev の密度定理より

$$\#T(r_0, t_0, X) \gg_E X/\log X$$

となるので, 以上の事実を合わせて補題が得られる. □

虚数乗法を持たない場合も, 同様にして次の補題が得られる.

補題 4.2 補題 4.1 と同様の notation の下で E は虚数乗法を持たないとし, p は 3 より大きい素数で E の p 等分点への Galois 群の作用から定まる Galois 表現

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\,(E[p]) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

は全射であるとする. このとき負の整数 D_0 で $(D_0, N) = 1$, $\epsilon = \left(\frac{D_0}{p}\right) \neq 0$ 及び $|b(|D_0|)|_p = 1$ を満たすものが存在すれば

$$\#\left\{0 < D \in S(X) \;\Big|\; \left(\frac{D}{p}\right) = \epsilon,\ |b(D)|_p = 1\right\} \gg_{E,p} \frac{\sqrt{X}}{\log X}$$

が成り立つ.

証明

ここでは虚数乗法を持つ場合との違いのみを述べる. l を素数とし $a(l) \equiv 0 \mod p$ とすれば, Hecke 作用素 $T(l^2)$ を考えることにより

$$b(l^2 n) + \chi'(l)\left(\frac{-n}{l}\right)b(n) + \chi'^2(l) l b(n/l^2) \equiv 0 \mod p$$

となる. このことから補題 4.1 と同様の手法により, ある正の整数 n_l が存在して

$$1 \le n_l \le [\Gamma_0(1) : \Gamma_0(Np^2 l)]/8 = \kappa(l+1),\ (n_l, l) = 1$$

かつ

$$b_0(n_l l) = u_l(n_l) \not\equiv \chi'(l) v_l(n_l) = 0 \mod p$$

となることが示せる.

さらに mod p の Galois 表現

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}\,(E[p]) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

は全射であることと Chebotarev の密度定理より

$$\#\{\, l : \text{素数} \mid l \le X,\ a(l) \equiv 0 \bmod p,\ l \equiv r \bmod t\} \gg_{E,p} \frac{X}{\log X}$$

となるので, 以上を合わせてこの補題が得られる. □

定理 1.1 は次の命題から容易に従う.

命題 4.3 $E/\mathbb{Q}$ を楕円曲線とし, その L 関数を

$$L(E,s)=\sum_{n=1}^{\infty}\frac{a(n)}{n^s}$$

とする. このとき $a(p)\notin\{-1,0,+1\}$ を満たす十分大きな素数 p に対し

$$\#\left\{D\in S(X)\,\middle|\,p\nmid D,\ \left|(1-\left(\frac{D}{p}\right)\alpha_p^{-1})^2L(E_D/\mathbb{Q},1)/\Omega_E\right|_p=1\right\}\gg_{E,p}\frac{\sqrt{X}}{\log X}$$

が成り立つ.

証明

$a(p)\notin\{-1,0,+1\}$ であり $\alpha_p\equiv a(p)\mod p$ なので, $1-\alpha_p^{-1}$ 及び $1+\alpha_p^{-1}$ は p-進単数となる. いま,

$$f(z)=\sum_{n=1}^{\infty}a(n)q^n\in S_2(N,1)$$

とし

$$g(z)=\sum_{n=1}^{\infty}(n)q^n\in S_{\frac{3}{2}}(N,\chi)$$

を定理 3.1 で与えられる保型形式とする. 必要ならば E を E のquadratic twist で置き換えることにより, $L(E,s)$ の関数等式の符号は+1 と仮定してよい. このとき Friedberg-Hoffstein [3] の結果により, 負の整数 D_0 で $(D_0,N)=1$ かつ $b_0(|D_0|)\neq 0$ となるものが存在する. このとき, とくに十分大きな素数 p に対し $|b_0(|D_0|)|_p=1$ となる. E が虚数乗法を持つときは, 補題 4.1 より

$$\#\left\{D\in S(X)\,\middle|\,\left(\frac{D}{p}\right)=\epsilon,\ |b(D)|_p=1\right\}\gg\frac{\sqrt{X}}{\log X}$$

であり, E が虚数乗法を持たないときは Serre [13] の結果によって, 十分大きな素数 p に対し, mod p の Galois 表現

$$\rho_{E,p}:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\mathrm{Aut}\,(E[p])\cong\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

は全射となるので補題 4.2 により, このとき

$$\#\left\{D\in S(X)\,\middle|\,\left(\frac{D}{p}\right)=\epsilon,\ |b(D)|_p=1\right\}\gg\frac{\sqrt{X}}{\log X}$$

となる. さらに定理 3.1 により, 十分大きな素数 p に対して $|b(|D|)|_p=1$, ならば $|L(E_D,1)/\Omega_{E_D}|_p=1$ となる. 以上からこの命題が成り立つことが分かる. □

最後に例を述べておく.

例 4.4 (cf. Tunnel [16]) 合同数の楕円曲線

$$E : y^2 = x^3 - x$$

を考える. pを5以上の素数とし Eはpで good ordinary reduction を持つ, すなわち $p \equiv 1 \mod 4$ とする. このとき,

$$\#\left\{D \in S(X) \,\middle|\, \lambda^{\mathrm{anal}}_{E_D,p} = \mu^{\mathrm{anal}}_{E_D,p} = 0\right\} \gg_p \frac{\sqrt{X}}{\log X}$$

が成り立つ.

参考文献

[1] D. Byeon, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields and congruence of modular forms*, Acta Arith. **89** (1999), 295–299.

[2] M. Chida, *A note on Iwasawa invariants of elliptic curves*, preprint.

[3] S. Friedberg and J. Hoffstein, *Nonvanishing theorems for automorphic L-functions on GL(2)*, Ann. Math. **142** (1995), 385–423.

[4] R. Greenberg, *Iwasawa theory for elliptic curves*, Lect. Notes in Math. **1716** (1999), 59–144.

[5] K. James and K. Ono, *Selmer groups of quadratic twists of elliptic curves*, Math. Ann. **314** (1999), 1–17.

[6] K. Kato, *p-adic Hodge theory and values of zeta functions of modular curves*, preprint.

[7] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. **135** (1999), 387–398.

[8] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $\text{Ш}_{E/\mathbb{Q}}$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), 522–540.

[9] V. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, **Vol. II** (1990), 435–483.

[10] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

[11] K. Ono and C. Skinner, *Non-vanishing of quadratic twists of L-functions*, Invent. Math. **134** (1998), 651–660.

[12] K. Rubin, *The "Main conjecture" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), 25–68.

[13] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[14] G. Shimura, *On modular forms of half-integral weight*, Ann. Math. **197** (1973), 440–481.

[15] J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes Math. **1240** (1984), 275–280.

[16] J. Tunnell, *A classical Diophantine problem and modular forms of weight $\frac{3}{2}$*, Invent. Math. **72** (1983), 323–334.